U-4 2-5

14-5

ARMED FORCES SECURITY AGENCY

107/50/TOPSEC/AFSA-14

Copy No. 6

From: AFSA-14

To: AFSA 02A7

DF 187-G

107/50/TOPSEC/AFSA-14

REPLIES BY MINISTERIALRAT FENNER TO QUESTIONS REGARDING CRYPTOLOGIC MATTERS

1. During his period of detention (September-December 1946) at the Hq 7707 European Command Intelligence Center, Oberursel, Germany, Wilhelm FENNER, former Ministerialrat and chief of cryptanalysis in the Armed Forces High Command Cryptologic Agency (OKW/Chi), wrote a lengthy report concerning his past career and his extensive experiences in the field of cryptology. This report was never issued in translation although an inadequate summary by Army Security Agency was issued as TICOM/I-206.

2. The present DF 187 Series constitutes a complete translation of FENNER's written report. The attached is the eighth and final part. It contains answers to several questions regarding cryptologic results and procedures. As in the case of the earlier parts pertinent notes from the TICOM files and from the memory of one of the original interrogators, Mary C. Lane, Capt. WAC, have been added.

3. The earlier parts of FENNER's report are:

DF 187	The Career of Wilhelm FENNER with Special Regard to his Activity in the Field of Cryptography and Cryptanalysis
DF 187-A	Organization of the Cryptologic Agency of the Armed Forces High Command, with Names, Activities, and Number of Employees Together with a Description of the Devices Used
DF 187-B	The Cryptanalytic Successes of OKW/Chi after 1935
DF 187-C	Relations of OKW/Chi with Other German Cryptologic Bureaus
DF 187-D	Relations of OKW/Chi with Foreign Cryptologic Bureaus
DF 187-E	Comments by FENNER on the Austrian Cryptologic Bureau and Former German Colleagues
DF 187-F	Remarks Made by Ministerialrat FENNER in Reply to Certain Questions of a General Nature

October 1950

Translated: RWP

Edited: MCL

[illegible] copies

[illegible] pages

DF-187-G

INDEX OF QUESTIONS

I. QUESTIONS REFERRING TO CRYPTANALYTIC RESULTS OR PROCEDURES

Page

II. QUESTIONS REFERRING TO CRYPTOGRAPHIC PROCEDURES

III. SECRET INKS AND MICROPHOTOGRAPHY

I. QUESTIONS REFERRING TO CRYPTANALYTIC RESULTS OR PROCEDURES

A. United States Systems

1. Who first solved the American strip system? How much information concerning this system was exchanged and with whom?

The question who first solved the American strip system might be answered most correctly by Regierungsrat Dr. WEISSER[1] and Regierungsrat SCHULZ.[2] To the best of my recollection the matter was as follows: by courier from Rome came a description of the solution of this cryptographic system which more or less astonished my unit because the problem involved was certainly one of the most difficult problems of cryptology. Chi did not think Rome competent to solve it independently but the character of

[1] Dr. Franz WEISSER was a member of Section 6 (England, USA) of Group a, Main Group B of OKW/Chi. He was interrogated by TICOM in 1946 and at that time gave the following account of the solution of the American strip cipher: (TICOM/I-201, p. 3)

> "After the Marine Bureau (FRANKE) had solved a system which was, (although the strip system was in the beginning rather primitive) a remarkable feat because it was a new kind of encipherment which had at first to be recognized, in May 1941 a log of strips covering all European traffics came in from Japan. After the introduction of the new system, solution work set in on a big scale in OKW/Chi by HUETTENHAIN and Dr. FRANZ, and in the Auswaertige Amt by KUNZE, rather in rivalry than collaboration. After several months work, the Auswaertige Amt succeeded in solving the system with the aid of Hollerith machines. Work for the next system was continued on a still bigger scale but without any success. From the Anglo-American department, Herr Helmut SCHULZ worked as liaison. He could have pushed the work forward, but he was hampered by the incapacity and vanity of Dr. FRANZ. A big help would have been Herr VOEGELE who had solved a similar system and who volunteered collaboration, which was refused as he was not considered competent, not being an academician. The small Finnish staff under Colonel HALLAMAA also collaborated quite effectively giving hints. Thus it found out that the systems used in different countries after some time emerged again in other countries. Later on, the strip system was applied in such a complicated way that work became hopeless. It was not abandoned, however, until the last phase of the war."

In addition to the above statement of WEISSER, there is available the detailed account written by Dr. FRANZ in 1946 and issued as DF 176.

[2] Dr. Helmut SCHULZ was mentioned by FENNER as a member of Section 6 (England, USA), Group b, Main Group B (DF 187-F). He has not been interrogated by TICOM.

the report made the impression of being absolutely genuine. Thereupon the problem was worked on at Chi and the work yielded results. About the same time very intensive work on the same problem was done at the Foreign Office, for a long time without success but later with success. I think therefore that the primary solution was found in Rome, whether independently or after securing certain basic documents remains for the present uncertain. Then Chi worked on the case carefully, finally the German Foreign Office and Helsingfors. Hence the fact of the solution of the strip system was known to Rome, Chi, the German Foreign Office, apparently to the Forschungsamt through the Foreign Office, Helsingfors and Budapest. Rome itself and Tokyo were not acquainted with the fact that solution had been successful because no furtherance of the work was expected as a result of informing these offices.

2. How did OKW/Chi obtain the code and deciphering tables of the Military Intelligence Code?

This has to do with the period shortly before the departure of the U.S. diplomats from Bucharest or Budapest. Summer of 1941 (?). OKW/Chi naturally was interested in reading reenciphered messages of the U.S. Government because it was to be expected that their content would be of moment. Attempts at solution failed. The work suggested a complicated reencipherment, apparently changing often. For between telegrams even of relatively close date there were no parallel passages (repetitions of groups of letters). It was suspected that perhaps there was a daily change as was characteristic for U.S.A. tables. Thereupon work on the traffic ceased.

One day I received courier post from Rome. In it was a U.S. code. The attempt to solve by this code the unsolved traffic was done only by sampling and naturally had no success. In any event the reencipherment could not be reconstructed. Some months later I received by courier post from Budapest some reencipherment tables, clearly of American origin. If I remember rightly, each of these tables had a serial number and an indicator group, then a horizontal plain alphabet and some substitution alphabets. According to the instructions for use, such a table was valid only for a limited time; I believe, several days. I then had an experiment tried to see whether the tables and the code went together. In about one hour my expert told me that the experiment had been successful; for OKW/Chi had messages fitting into the period of validity. From this time on the messages were read even when there were no tables available. The break-in was accomplished by using stereotype telegraphic phrases. I think this system was also used by the U.S. Military Attache in Cairo. The reencipherment material was photostated. I was told it had been removed temporarily from the baggage of a U.S. Ambassador departing from Bucharest (?) Budapest(?). (My assumption is as follows: When the U.S. Ambassador was leaving Bucharest before Roumania's entry into the war, he had a stay of some hours in Hungarian territory. At that time his baggage, which may not have been sealed, was opened and the reencipherment was photostated.) The originals were supposed to have been returned promptly and unnoticed. That is the story which was given me. I do not know whether it corresponds with the truth. If this system and not the strip cipher was used by the U.S. Military Attache in Cairo down to the battles around Tobruk but was then replaced, that may have been in connection with the introduction of a cipher machine. However the War Department may also have heard something to the effect that this system had been compromised.

Regarding this affair Regierungsrat Helmut SCHULZ probably is better informed.[3] In June 1945 he was in Weihenkirchen near Bad Aibling.

B. Russian Systems

3. Give details concerning the Russian Army maneuver code which you said was broken in 1930.[4]

---

[3] SCHULZ was not interrogated by TICOM, but WEISSER's statements correspond to FENNER's. WEISSER also adds some notes on the method of solution. (TICOM/I-201, pp. 1-2).

[4] Apparently the question was based on a remark of FENNER which has not been recorded in the reports of interrogation. Elsewhere in his reports, FENNER seems to have recognized only OKK-5, 6, 7, and 8 as [illegible] worked on by OKW/Chi. Cf. the oral interrogation (TICOM/I-201): "Russian Army 4-figure codes, known as OKK (Obschchij komandir kod) 5, 6, 7, and 8 were read from 1939 tc 1941. OKK-5 was captured after they (OKW/Chi) had read it, and they also captured copies of 6, 7, and 8." Cf. also the written report of FENNER (DF 187-B): "From their first appearance to the summer of 1943 the cryptographic systems "OK" and their successors were worked on and solved. I think the first system of this kind was "OK-5". I am sure that OK-6 and OK-7 were solved and later, I believe, OK-8 as well. If I remember rightly, these were 4-digit codes with partial reencipherment by 2-digit substitution tables."

Chi solved Russian Army systems currently from the First World War on and went through the entire development from the simple substitution systems to the codes reenciphered by additive. But what system the Red Army used during its maneuvers in 1930 I cannot tell. I have become acquainted with hundreds of different systems but have carried as few as possible around in my head to such a degree that I could give any information regarding them 16 years later. Judging by the time, it must have been OKK-1 or OKK-2 because OKK-1 was supposedly compiled in 1929. I presume it was a 3-digit code which at best was reenciphered with a partial digit substitution table. Such a development would fit in best at that time.

4. METTIG has stated that the Finns sent Russian 5-letter traffic to OKW/Chi.[5] Do you know about this traffic? When was Russian 5-letter traffic first noted by the Finns or Germans?

METTIG was with the Army Cryptologic Agency (OKH/In 7/VI) before he was transferred to OKW/Chi. What he reported regarding 5-place Russian traffic with the cryptologic service of Finland clearly refers to METTIG's activity with OKH/In 7/VI. Furthermore there is an error here: Soviet Russia had long since accommodated itself to international conventions and, as a matter of principle, sent all radiograms in 5-place groups. Therefore, there never were any Soviet Russian radiograms which would have been characterized by the fact

[5] FENNER, it is noted, rightly takes exception to this statement. TICOM/I-78 is the interrogation of METTIG on the history and achievements of OKH/In 7/VI, the Army Cryptologic Agency, which he directed from November 1941 to June 1943. TICOM/I-96 is the interrogation of METTIG on the history and achievements of OKW/Chi, of one of whose groups which he was the head of from December 1943 to the capitulation, May 1945. In TICOM/I-78 METTIG states that a copy of the Russian 5-figure code was given to OKH/In 7/VI by the Finnish General Staff during the Russo-Finnish War. He also stated that OKH/In 7/VI successfully solved in April 1942 the new Russian 5-figure code, and that from 1942 on all 5-figure traffic was collected at Loetzen (location of the Army cryptanalytic group for Russia) and that some of it was currently read. FENNER is therefore correct in referring this statement to OKH/In 7/VI rather than to OKW/Chi. In his discussion of the relations of OKW/Chi with the Finnish Cryptologic Service, FENNER states that "in contrast to Budapest, it was not so much the intercepts from Helsingfors which played the decisive role as it was the exact and successful cooperation of OKW/Chi and the Finnish Büreau in the field of practical cryptanalysis" (DF 187-D).

that they had 5 places in the group. Thus even the cipher OKK-5 and its successors were sent in groups of five. When METTIG came to OKW/Chi about the fall of 1943, the cryptologic service of Finland had no contact with OKW/Chi in the field of Russian Army systems, but was working with the Army Cryptologic Agency, where I became acquainted with the Finnish officer, MIEK-OJA, whom I have mentioned elsewhere.[6] The cryptanalytic service noted 5-place groups even during the First World War. When the cryptologic unit of the Reichswehrministerium started work, the Russians were again using 5-place groups on the radio as a rule. And when Finland began work in 1927 at the latest, the Russian Army radio traffic was in 5-place groups almost without exception. Deviations were an exception and probably a punishable error.

5. What cipher machines were used by the Russians and the Balkan armies or governments? When were they used? Were any captured? Do you know anything about Russian machines of a type similar to the T-52? What do you know about Russian agent systems?

I know nothing about Russian secret teleprinters and have never seen such a machine. I do not know anything sure about Russian agent traffic because I never had in my hands any actual traffic. I have received single statements of deserters and prisoners. Inasmuch as there was no traffic at hand I was not able to check their statements. Ostensibly the cryptographic systems of Soviet Russian agents were based essentially on the use of a 2-digit substitution derived from a prearranged indicator word. This had no variants and was reenciphered by an additive sequence which was derived from a prearranged sequence of digits. For example: Indicator = STALIN. Then С= 01, Т = 02, А= 03, Л= 04, И = 05, Н = 06, Б = 07, В = 08, Г = 09, Д = 10, Е = 11, Ж = 12, З = 13, etc., following the Russian alphabet. For reencipherment the birth date 22.10.25 might have been used. In this primitive case this 6-place number would merely be added "symbolically",

[6] DF 187-D, p. 4.

i. e., modulo 10, to the text obtained by substitution. In other cases the birth date was used to derive the additive sequence. The agent would then derive the following sequences of digits:

221025.1 = 221025

221025.2 = 2220410*

221025.3 = 6630615

221025.4 = 8840820

221025.5 = 1010501025

221025.6 = 1212601230

221025.7 = 1414711435

etc.

And from the sequences of digits comes the additive sequence:

22102522204106630615884082010105010251212601230141471l435................

43127744245162936763624802111155112763338613531555182578................

This additive sequence was added symbolically. Reports on cryptographic systems of this kind were merely noted but not worked on in my unit because that would have exceeded the bounds of my activity. On the other hand, I assume that First Lieutenant Dr. VAUCK worked on these rather carefully, although I cannot recall that he broke any Russian agent systems after the fall of 1944 when he was transferred to my group. The example I have given is only one of the vast number of variants of this principle. In case cryptograms of this kind had appeared, they would have had to be worked on as though the additive were unknown, since only after solution could the construction of the additive itself be discovered.

The sending in of single ciphers of this kind, where it was impossible to prove whether they were genuine or not, was of value only for information, the practical value was virtually nil. For the rest, I should like to refer in connection with this question to the ex-Soviet Russian, Colonel SACHAROV, interned in Haus Alaska, who knows the Russian agent system thoroughly

* Translator's note: Error, which is repeated below.

and can perhaps give information regarding the Soviet Russian agent ciphers.[7]

C. Jugoslav Systems

6. HERZFELD of OKH/In 7/VI has stated that instructions for a Jugoslav additive system were found in a cave near Drvar. Have you seen this material? What became of it? Can you describe the Jugoslav additive systems?[8]

I assume that the Jugoslav army systems are involved. I am not acquainted with them and the event mentioned was not known to me; nor do I know what became of the material from OKH.

D. Polish Systems

7. Describe the development of Polish systems after the First World War.

When, after the First World War, the new Polish State had to supply its diplomatic representatives abroad with a means of making confidential and secret reports and of receiving orders with like classification, recourse was had to means known to all civilized people since the 50's of the last century: a cryptographic system which could be sent by telegraph. So it was not surprising that soon secret dispatches were being conducted to their destination by cable and radio, dispatches bearing the addresses "Polmission" "Polextern," "Militpologne" - whose meaning requires no explanation.

When the Cryptologic Bureau of the Reichswehrministerium began work on these messages, a few government cryptographic systems might have been

[7] See DF 187-F, p. 19 for FENNER's discussion of the work of Dr. VAUCK, who was head of a unit working on agent traffic. As was stated in DF 187-F, note 38 (p. 22) during his period of interrogation, FENNER was interned in the European Command Intelligence Center (ECIC) at Haus Alaska, a private residence at the Center which was reserved for important persons under interrogation. SACHAROV was interned there at that time and was being interrogated by the Director of Intelligence, European Command. No TICOM interrogation of SACHAROV was undertaken.

[8] The question was based on HERZFELD'[illegible]se) in which he said that as a result of a German parachute operation near Drvar against the Jugoslav leader, TITO, a large mass of Jugoslav cryptographic material was left in one of the Drvar caves by TITO's "Centralni Buro za Sifrovanje". Among the cryptographic papers thus left were instructions for a new "key" about which there had been much talk in the reports of the early months of 1944. FENNER is here queried about his knowledge of this important cryptographic find.

introduced and replaced, so that we can say nothing about them. It is also possible that the messages which Chi first studied early in the 20's of this century still represented the type of the first Polish Government cipher: 5-digit groups with parallel passages within the same message and among telegrams of the same date; on the other hand, no parallel passages among telegrams of different days. The length of the parallel passages was always 4 or a multiple of 4 so that there was no reason to doubt that the basic system was 4-place, i. e., a 4-digit code. The parallel passages collected for a study of the reencipherment showed affinities, the regularity of which could not be disputed: if, for instance, on 1 October there was a parallel passage 4354 7355, then on 2 October there would be found the parallel passage 1061 9066, and likewise, if yesterday a frequent group had the appearance 8579, today a group would appear reading 2693 and having about the same frequency, i. e., would occur about as frequently percentually. On the basis of this observation and dozens of confirmations it was natural to assume that a 4-digit code had been reenciphered by a simple substitution table which might have appeared as follows when partially solved:

2 October	
0 =	
1 =	
2 =	
3 =	0
4 =	1
5 =	6
6 =	
7 =	9
8 =	2
9 =	3

Work on the traffic of each day led to the same phenomena. The correctness of the assumption was thus confirmed and the next step could only consist in making all the still heterogeneous traffic homogeneous [illegible] as if for reencipherment only one and the same substitution table from among the arithmetical conceivable 10! - 1 permutations had been used. This procedure is called reduction to a relative basic code. It is accomplished by comparing the largest and most accurate batches of daily traffic available, regarding one of them as "plain", i. e., as not reenciphered, while the others were reduced to this. The work of reduction itself ran along in schematic fashion. The method is probably the same among cryptologists of all civilized countries, hence a hint suffices.

The following page shows a section of the count of the day's traffic taken as basic code (black), 4-digit; the count of the second day's traffic, also 4-place naturally, (red), and the count of the third day's traffic under the same conditions (blue). If black 1365 is the most frequent group in batch one and 0128 the most frequent group of batch two, while 5431 is the most frequent group of batch three and at the same time groups 1456, 0682 and 5713 might correspond, we can already carry out the following reduction:

Black	Red	Blue
0		
1	0	5
2		
3	1	4
4	6	7
5	8	1
6	2	3
7		
8		
9		

It is obvious that by other comparisons supplementary values will be found so that if enough traffic is received the messages can be reduced to "black" to supply initial material for breaking the code.

Thus the problem of the 4-digit code reenciphered with a simple digit substitution table was solved, but at the same time it was proven that such a system does not satisfy modern security requirements.

Now if a system had been selected which was not in and of itself secure enough to safeguard state secrets, the solution of the daily changing reencipherment was further facilitated by the fact that Warsaw itself introduced a facilitation which was not a necessary consequence of the system but was merely the result of thoughtlessness and convenience. In comparing the successive daily keys of a month, certain systematic sequences were found which made it possible to solve the reencipherment of days when traffic was so light that its statistical picture would have been indefinite and also to derive the substitution tables even before a single telegram had been received for the day in question.

Obviously the reencipherment tables for a month were printed on a single sheet of paper. The official charged with the production of these tables made the job easy for himself and neglected the one thing which would have been the only correct thing in such cases, namely the use of the "lottery system" in order to exclude any systematic character, including involuntary but psychologically comprehensible ones. So the tables looked somewhat as follows:

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	6	9	3	9	1	5								4	4	2	2	0		3		5	1								
1	0	3	9	1	6	1	5						4		2	4	0	2	3		3	1		1							4
2	3	0	1	3	5		1	5				4		2		0	4	3	2	0	1	3			1					4	
3	2	1	0	5	3			1	5		4		2		0	5	3	4		1	0		3			1			4		2
4	1	2	5	0	9	3			1					0					1												
5	4	5	2	8	0		3			1			0					1													
6	5	4	6	2	7	0		3			1	0					1														
7	9	6	4	7	2		0	4	3	2	0	1				1															
8	7	8	7	4	8	2	4	0	2	0			1		1																
9	8	7	8	6	4	4	2	2	0	3	5	5																			

Systematic features like this and others occurred by the hundreds and constituted the rule while unsystematic tables were the exception. And even though these systematic features could only be regarded as partial, nevertheless in countless cases they facilitated the work of the cryptanalyst because, if part of the month's table was solved, he already recognized approximately how the table for the following day would appear.

When this system had been used for some years, it was replaced without warning by a new 4-digit code which was reenciphered by means of additive sequences. (I cannot give the date without reference to an archive, but do know that the new system had already been in use for some months at the time of the so-called mail box conflict in Danzig.)

Critical examination of the secret text, i. e., attentive scanning of the new messages without preparing any counts, gave a very different picture. The number of parallel passages had become very much less, their length was 4 or a multiple, the basic code was therefore clearly 4-place, which was again confirmed by the fact that the interval between parallel passages had remained a multiple of four. A frequency count which was now made yielded an absolutely colorless picture, in other words there must be a reencipherment which permitted virtually every digit of the secret text to occur equally often percentagewise. Since an additive sequence of sufficient length is known by experience to produce such an effect, it was assumed with great probability that an additive sequence was involved. From the occurrence of parallel passages the so-called phase or period was recognized as 4-place and the next task was to seek out enough homogeneous material that had been reenciphered with one and the same additive sequence. The introduction of the additive sequence meant a great advance cryptographically. But again Warsaw lulled itself to sleep in a feeling of security which was subjectively intelligible but which could not stand up against objective critical study. The additive was short and was always in use for so long a time that enough messages were accumulated regularly to be able to solve the problem successfully. For this purpose use was made of a method which is surely common to all cryptanalysts in modern civilized countries, the difference method, which from an arithmetic point of view consists in the fact that like differences of two groups standing in the K^{th} position (of the additive sequence) and in the $K + n^{th}$ position (of the additive sequence) apply to the same code groups.

```
..........k.........          k+n...........
          3456                4567
          ....                ....
          ....                ....
          7322                ....
                              ....
                              8433

Diff.     4976                4976
```

However that is also the difference between the plain code groups 2345 and 6211.

Since only in very rare cases is a reduction to the true basic code possible, reduction is generally to a relative code until enough homogeneous material is assembled to permit an attempt at the breaking of the code. The Polish exchange of messages was always so lively that the necessary amounts of traffic were always available. Thus again the security of diplomatic state secrets was not high enough: In spite of the use of a system which was modern in and of itself the mistake had been made of sending enough traffic with short additive sequences to compromise the system itself.

DF 187-G

It must be assumed that later on a competent critic appeared in Warsaw who recognized the disadvantages of this system and called attention to them, possibly an officer (Lieutenant Colonel SZCZEZINSKY ?). For the next improvement consisted in lengthening the additive sequences. The use of a 4-place number series was due of course to a want of imagination: 40 digits are an integral multiple of 4, when the additive sequence has run out, the next group begins again with the first digit of the additive; on the other hand an additive series of 37 places used with a 4-digit code would not repeat until after 4 x 37 steps, i. e., would have practically 148 positions. When Moscow became aware of this, the additive sequences were derived from this point of view; then however it was not long before longer series appeared which had over 200 digits. That was an advance for it happened again and again that telegrams were dispatched which were shorter than the additive sequence and when traffic was scant entire messages remained incapable of solution. It is a well known fact that a thing which is theoretically correct must also be correct in practice. If there are contradictions nevertheless, then either the theory is false or a mistake has been made in practice. The theory of the additive sequence requires of course that the additive shall not always be applied at the same point to the intermediate text (code text before it is reenciphered). In practice however it was often different! The cryptanalyst got the impression that the additive sequences of the code clerks were kept in the table drawer and by force of habit were applied to the intermediate text at exactly the same point as in a number of previously enciphered messages. At the time this was observed an additive sequence was still used for a relatively long time, - I cannot say today how long, but in any event for so long a time that as a rule enough traffic was sent to make possible solution of the reencipherment. In this connection it was indubitably a mistake that between Berlin and Warsaw, for instance, the same additive sequence was used. Later, however, at least one defect was eliminated: the period of validity of the additive sequences was shortened. The consequence of that was that the amount of solvable material disappeared more and more and more, that is ever fewer and fewer secret telegrams could be deciphered. However, Warsaw could not make up its mind to give this system, which in and of itself is excellent, that stability in practice which it possesses in theory. And it was not until the final months before the outbreak of the war that that level was obtained which the Polish Government ciphers might have reached as soon as the additive sequence was introduced: in each direction on each link the additive sequences were different, that is to say, in the traffic from Warsaw to London the same additives do not occur as a matter of principle as in the traffic from London to Warsaw; the sequences themselves are so long that they do not reappear even once within a message in most cases; the sequences have such a short period of validity that only in isolated cases is enough traffic available to be able to solve the reencipherment! For months before the outbreak of the war Chi was therefore unable to solve a single Polish diplomatic message. Thus Warsaw had satisfied the requirements of a modern governmental cryptographic system: its nature was known, its weaknesses were known, but it was used in practice in a manner corresponding to its theoretical value and consequently protected the secret from all unauthorized tampering.

When the war broke out and the Polish Government-in-Exile began receiving and sending messages, it soon proved that what had once been learned had not been forgotten. They stuck to the reencipherment by additive sequences. And corresponding to the impossibility of preparing and distributing under the prevailing circumstances as many additive sequences as were necessary, they chose sequences which could be derived from extensive tables. Surely the Government-in-Exile knew that this method is dangerous if the period of use is long. But under such difficult circumstances it may have been beyond the power of those responsible to create anything better, for the disadvantages of these really rigid tables could be recognized in the course of time by a cryptanalytic unit. Thus Poland could not prevent large numbers of these messages from being read. Basically the replacement of the basic system and of the additive tables did not change this at all. But it would be wrong to assume that the solution of these cryptograms was easy. Weeks always passed before homogeneous traffic in sufficient quantity could be accumulated and in view of the personnel shortage at Chi it was not possible to work on these systems according to the old peacetime methods, i. e., simply by hand. Instead, in order to have success, cryptanalytic aids, such as differencing machines and Hollerith machines, had to be employed if decipherment was to have any practical value whatsoever. However, precisely this circumstance does not argue in favor of the system selected because the modern cryptographer must count on the fact that the modern cryptologist will attack his systems with machines designed to save labor. And the rule remains, that every cryptographic system has its innate degree of security which must not be overburdened. When this case will occur cannot usually be foreseen when a system is introduced, and far more frequently than a layman will assume the time of exposure cannot be recognized by the user of a system because he very rarely has a chance to survey the "total consumption" of a system. The system known as "Militrologne" was likewise worked on and its reencipherment was solved. I can only give its characteristics today with reservations: 4-digit code, reenciphered by a simple digit substitution table, hence no problem in and of itself! Here the difficulty lay in another field: the amount of traffic available was not by any means adequate for solution of the code. So in this case too everything was known but success was not achieved because the innate degree of security of the system had not been reached, let alone exceeded.

That Warsaw had not been idle and had not rested on the laurels of the infinite additive sequences which had become virtually incapable of solution, was proven by some captured material turned in: military code books composed in several languages and designed for communication in Polish, French and [illegible] during the preparation for and execution of large-scale operations. Also from other code books and prepared reencipherments one could not fail to recognize that Warsaw was taking pains to make adequate preparation for any eventuality. Even the exterior of these documents showed that attention had been paid to the choice of paper, binding and makeup, so that a certain high standard had to be assumed for the entire cryptographic work of the government.

Regarding the philological solution of the Polish codes it may be stated that it was not made easy by any means. This assertion becomes quite clear if we compare with France whose diplomatic codes were also usually four place. Whereas the Frenchman carefully encrypts every stem and every ending and insists on accuracy in grammatical form, the Pole prefers the opposite practice: often he only gives the stems and assumes that the decoder will have no difficulty finding the correct meaning on the basis of his political knowledge, in fact that he will not even have to look for it as a rule. That is all right for him but the decoder is very much retarded in his work of interpretation by this method of encoding. Thus, while a normal French diplomatic 4-digit code can often be read after the recovery of some 1,500 groups, in Polish even 25,000 groups were not enough! This fact deserves consideration as a proof of how important it is to assure by the very process of encoding that additional difficulties arise for the enemy cryptanalyst.

However it holds true for the cryptographic work of the young Polish State that even when advisers were surely not wanting, the development of cryptography goes ahead not by leaps and bounds, but organically related to the organism man, whose spiritual eye can, it is true, in fortunate hours see to great depths, great heights and far distances but with this vision cannot force its dear fellow man to do what is rational.

8. Was any examination undertaken of Polish traffic connected with the Polish Lublin Government? What was known of this traffic?

I cannot say with certainty I ever saw radiograms of the Polish Provisional Government in Lublin. However, I assume that among the numerous decrypted Polish messages there were some of the Lublin Government. In type these can only have been substitutions with additive reencipherment, whereby the additive was [illegible] from a table. It would be best to question the former detailed official BERNDT[9] about this, otherwise Dr. HUETTENHAIN[10] who was in closer contact with BERNDT regarding the reencipherment than I was.

[9] Edgar BERNDT was head of Section b 16 (Poland) of Main Group B of OKW/Chi. BERNDT was never interrogated by TICOM.

[10] For FENNER's opinion of HUETTENHAIN see DF 187-E, p. 16 and note 7.

E. Finnish Systems

9. Did OKW/Chi ever attempt to solve Finnish systems? What kind of systems were they? What success did OKW/Chi have?

Dr. LUETJEN,[11] employed in my unit, undertook investigation of some Finnish Government telegrams around 1940, without achieving any results. Since repetitions were not found in the texts studied, it was assumed that some form of transposition was involved. The question was not studied more closely because the work on other telegrams (Bulgarian) was more important.

F. Unidentified Systems

10. Have you heard of 30-letter traffic with indicators which seem characteristic of one-time pads?

Yes, once, as far as I can recall, I talked with PASCHKE[12] of the Foreign Office about one-time pads, radiograms 30 letters long (constant), with some indicator words or other. We did not know what to do with such messages, however, because we did not even know their nationality. I should guess that that was late in 1943 or early in 1944. However at that time, with our reduced personnel, we already had so many worries trying to keep up the diplomatic decryptment that we could not devote ourselves to work on traffic which lay outside the limits of our assignments.

G. Machine Systems

11. What do you know about the Italian Olivetti teleprinter? Have you ever seen it?

No, I have never seen the Olivetti cipher machine. However, it is known to HUETTENHAIN, to whom it was shown. In HUETTENHAIN's opinion the machine had not yet been sufficiently developed from a technical point of view and it delivered a secret text which did not afford adequate security against cryptanalysis, provided the machine was known. That is to say the constants of the

[11] See DF 187-A, p. 9 where Dr. LUETJEN is mentioned as a member of Section 22 (Bulgaria) Group b, Main Group B. In this list Dr. LUETJEN's military rank is given as private (Soldat).

[12] Dr. Adolf PASCHKE of the Foreign Office Cryptologic Bureau. See DF 111 for the written interrogation of PASCHKE.

machine outweighed the variables of the machine in their effect.

12. You stated in oral interrogation that you believed the Olivetti machine had been shown to the United States Navy.[13] How did you know this? Give details.

I never said so! I told the interpreter that HUETTENHAIN had seen the Olivetti cipher machine in Italy. Because of the preponderance of Italian naval officers HUETTENHAIN got the impression that the Olivetti had been pushed by the Italian Navy, consequently not by the Italian Army. I reported on that because Chi had to do only with General GAMBA, i. e., with an officer of the Italian Army, while Chi had no contact with the Italian Navy! But the American Navy had nothing to do with the matter. Hence a pure misunderstanding.

13. What do you know of the history of the "Grosse Teknik"?

The Swedish engineer, Boris HAGELIN, developed late in the 20's or early in the 30's a cipher machine which, as I assume to be known, is based cryptographically on the principle of the virtually infinite Tritheim. He accomplished this by a number of gear wheels whose ratios were "prime" to one another (11, 13, 17, 19, 21, 23) and so-called pin wheels (<u>Bolzenraeder</u>) whose purpose was to cause this period itself to run off in irregular skips. A third aggregate, the so-called "basket" had the task of effecting a substitution of the alphabets in the machine. The device, which was some 20 cm x 15 cm x 8 cm in size, was developed as a "tape printer". Pressing a hand lever moved the entire mechanism by a certain "number of steps". A letter wheel had to be set with the left hand, then alongside in an opening the corresponding cipher-text letter appeared after the lever was pressed. This device, which was excellent from the cryptographic standpoint, had the disadvantage of working relatively slowly.

[13] Unsatisfied with the answer given by FENNER to the previous question, the interrogators posed this question in the hope of "pinning" down FENNER to a more complete statement. This question was based on the statement recorded in the oral interrogation (TICOM/I-200, p. 12): "He /FENNER/ had heard of the Olivetti teleprinter, but had never seen it and could not describe it; he thought it was 'not yet ripe.' He believed the Italians had later shown it to the U.S. Navy". FENNER here insists that the last statement rests on a misunderstanding on the part of the interpreters.

DF 187-G

Around 1933 HAGELIN offered his patents to the German Wehrmacht but the sale did not come about because HAGELIN supposedly was asking over one million marks. On a later visit he told me himself that his devices were being built in France under license.

A few years later it was obvious from public advertisements that HAGELIN had improved his machine: he had introduced a keyboard similar to that of a typewriter and had, so far as I recall, a strictly mechanical type and an electro-mechanical type. Since Chi and the Ordnance Branch had ideas of their own after 1935, one was content with the knowledge at hand and did not purchase any devices of this type for study. (The purchase would have been very difficult due to exchange regulations).

In the summer of 1940 some cipher machines were captured in the West which were recognized as automatically printing, electro-mechanical Teknik devices. The base was about 40cm x 40cm, the height I should guess was 15 cm. I know of two machines but assume that the Ordnance Office (Wa Pruef 7) may have kept some. No device was whole. I cannot tell today whether they were so-called page printers or tape printers, or whether they printed the plain-text letters as a check (on the cipher text). That was purely secondary as far as Chi was concerned. On the other hand it was important that for deriving the actual cryptogram the elements of the already known "little Teknik" were used, namely:

1. Gear wheels with the number of teeth prime to one another.
2. Pin wheels.
3. Basket with riders.

What was new was the fact that to accomplish the letter substitution wheels had been introduced after the manner of the wheels in the German Enigma. As power source a dry battery was [illegible] I think there was a cable to enable taking transformed current from the light circuit. I am no longer sure of the mounting of the individual parts and their effect. (Since there was apparently no traffic from these machines and since I could never find out whether they had been used by the English or the French, the purely cryptologic interest was exhausted.) However, the cryptanalyst and the machine specialist were interested in a small cylinder which was missing in every machine. As I recall it this must have been about 4 cm long and about 3 cm in diameter. It was placed between certain electric poles after the manner of a small Enigma wheel and in our opinion signified an additional individual security factor. I no longer know how many poles this body had on its faces. However, I assumed at that time that there must be a very great number of such supersecret wheels, and that the device would not function at all without such a wheel was clear. Hence the machine could be left standing open on the table but as often as it was used such a wheel had to be inserted by the person in charge (officer, official). I requested that a search for such wheels be made in all depots and factories of the occupied territory, but got no results. Consequently no machine could be put in a condition where it could be studied and used experimentally.

However, one thing was clear to me and to my associates Dr. HUETTENHAIN, graduate engineer ROTSCHEIDT, and MENZER: that HAGELIN had won a good head start and that the device must be theoretically very good for use in a fixed installation. We could set up no rule for the solution of the individual Teknik message; of course we did not know either whether the device has any technical defects and is "subject to disturbances".

This device did not reach us in time to have any stimulating effect on our own ideas. The machines we had were taken along by MENZER when he and his group were separated from us in 1944; what became of them I do not know. MENZER tinkered around on one device but I do not believe he ever got it operating properly. I should surely have heard of it.

Judging by its appearance the machine was undoubtedly built in a stable dependable fashion and could be called a piece of good clever workmanship.

14. What do you know about French machines, in particular, the B-211? Were any captured? By whom were these machines studied?

There were some captured Hagelin B-211 at Chi. Same size as the small Hagelin. On the letter wheel in the left corner the letter W was missing, as far as I recall. I have already described the basic principle of the internal structure in another place. No other French cipher machines are known to me, for the big Hagelin which printed the cipher text by means of a keyboard and type was probably used by the English. Regarding the possibility of solving B-211 messages the erroneous idea has been expressed that OKW/Chi solved the B-211 messages. That is not correct. I merely know from conversations with HUETTENHAIN that under certain circumstances the B-211 yielded cryptograms which could be solved. However I cannot tell you anything about these conditions because I am not adequately informed. Perhaps OKH pursued this problem with greater care and actually forced a few solutions.

DF 187-G

II. QUESTIONS REFERRING TO CRYPTOGRAPHIC PROCEDURES

15. Describe the German Enigma, the SZ 40, 42, and the SG 41. On what principle did they work? How secure were these machines considered? Who could best know about these matters?

Many hundreds of the Enigma used by the German Wehrmacht were lost. Therefore I am firmly convinced that some are in American hands. If I were to try to give the desired description without having one before me, I should run the risk of being incomplete or even erroneous in my statements. It might therefore be more to the point to apply first to American experts. The devices 40, 42 and 41 I cannot describe at all because my knowledge of such devices is not adequate. Those who were occupied with these devices include: Dr. HUETTENHAIN and MENZER of my unit, also graduate engineer ROTSCHEIDT, LIEBKNECHT (Dr. Ing.?) and Dr. LOTZE of the Ordnance Office (Wa Pruef 7). Possibly Georg SCHROEDER, former Ministerialdirigent in the Forschungsamt can give information regarding these devices since, so far as I know, he was a member of the commission for devices of which HUETTENHAIN was chairman. Probably HUETTENHAIN can give the best information.

16. Describe the weaknesses of the Enigma discovered by MENZER. How were these weaknesses counteracted? Was the discovery of these weaknesses used in the examination of the machines of other countries?

I had no active part in the latest development of the Enigma. In case a new model was introduced during the war I am no longer in the picture. But, nevertheless, it is probable that nothing essential was changed in the basic principle.

I assume that at least one undamaged model of the Army Enigma is to be found in Washington since many machines were lost. If all the bulbs still light up, I suggest making the following experiments:

1) If in any random wheel positions key "A" is pressed and if at the same time the lamp field "K" lights up, then in the same position pressing key "K" will light lamp field "A". Experiments with the other keys would always lead to the discovery that two letters are always related "reciprocally". From this it follows that in the system of the

Enigma there are "reciprocal substitution alphabets." Now with 26 letters in the alphabet the number of substitution alphabets is 1 x 2 x 3 ....25 x 26 = 26! On the other hand, the number of reciprocal substitution alphabets with 26 letters in the alphabet is only (26 ÷ 2)! = 13! This is a weakness inherent in the machine and one which cannot be eliminated because it is conditioned by the construction of the machine, its circuits and switching. But in the entire Enigma system only 13! different substitution alphabets occur. Hence, if one succeeds in solving one of these alphabets, it becomes obvious even during solution that each value solved yields two values. For instance, if cipher "A" = plain "K", then in this position cipher "K" necessarily is equal to plain "A". In the final solution this circumstance naturally facilitates matters, i. e., it is a weakness.

2) If a machine is available in which three wheels turn between a fixed wheel at the right and at the left, then the whole maze is run through after $26^3 - 26^2$ = 16,900 steps. For due to the rests (Rasten) on the bodies in the form of a circular saw, the progression was not like that in a numbering machine but instead 26 x 26 substitution alphabets are skipped. This leads therefore to a shortening of the period even though the progression suffers a distortion in this way.

3) Assuming the case that a machine is allowed to be used for an entire day with the same wheel position and rest position (Rastenstellung) and all messages are enciphered in exactly the same wheel position, for instance all beginning in the position 010101, then the solution of such messages calls for little effort if some 70 are available while solution is possible even with fewer messages, assuming that the cryptanalyst already has some experience and training. In order to avoid any such piling up of messages at one point in the wheel period, all messages really ought to be distributed quite evenly over the period. However, that can only be achieved in traffic controlled by a single station, not

otherwise. It is most appropriate to instruct the stations to take random message keys because it is then probable that the day's traffic will be distributed over the entire period so evenly that no dangerous piling up will occur.

4) Nevertheless this security by no means satisfied current demands. For nobody can tell how great the daily volume of traffic will become in a future war, all estimates of this kind were absolutely without real basis and therefore inadequate. The ideal would have been to be able to undertake currently a permutation of the circuits! E. g. by interrupting the leads of the fixed wheel at the right and constantly shifting the pole connections, that is if one could make the most varied connections between them. This idea led to the development and introduction of the plugboard (Steckerbrett) with 26 jacks in the front of the machine. When the jacks are not bridged over, the machine works in normal position so to speak.

5) If I key a message in a predetermined position without bridging these jacks and then key the same message once again in the same position but using one bridge, uniting - let us say - jacks "A" and "K", then the two cipher texts will be alike for the most part, i. e., just this discovery by itself shows that a single bridge is by no means adequate to cause in the substitution alphabet sequence of the period a distortion which cannot be recognized. Even when using two or three bridges there are not sufficiently great changes to allow us to say that the device has now become secure. Since in calculating the bridges combinations are encountered, the maximum - so far as I can recall today - is found not with 13 bridges but with a smaller number.

6) There is nothing so erroneous as to assume regarding an opponent that he will not notice weaknesses of a cryptographic system and therefore fail to make use of them to the full. Consequently Chi assumed as a matter of principle that the Enigma would fall undamaged into enemy hands along with the instructions for its use and at least a few keys. It was also obvious that the enemy would likewise have radiograms. It was

also self-evident that accident, regarding which one can never tell mathematically when it will occur but merely knows that it occurs, will some day give the enemy a possibility of deciphering individual Enigma messages, even if the machine is used correctly. What really had to be guarded against was that the enemy should read the Enigma messages currently! In this connection it was also clear to Chi that Enigma messages with the same or similar key positions could not fail to contain so-called parallel passages, which in turn were a weakness inasmuch as by their aid affine messages could be worked on with success: one merely needed to superimpose messages with parallel passages correctly, then all elements in a column were probably from one and the same substitution alphabet! For example

```
.......aldefro...........xdert...........cafhjk........
.......ligtfde...........xdert...........vgftrea.......
.......aldfrcc...........................bhiklog.......
.......xzzefrc...........................cafholj.......
```

Here it was only necessary to remember that, due to the dropping out of certain alphabets, the cipher elements of all columns across the entire width did not really need to come from the same reciprocal substitution alphabets. For this reason the possibility of the occurrence of such parallel passages should be avoided! Parallel passages arise through the use of like letters at identical positions in the period. The identical sequences of letters result from the choice of the same word. The military language is poor in words! Again and again we meet the words: Gegner (enemy), feindlich (hostile), Angriff (attack), Munition (ammunition), etc. And in these words the most frequent German letters also occur, e. g.: e,n,i,r,f,t,u,d,a,h,b. If bridges are introduced it is desirable to disturb these frequent letters.

7) Now the number of bridges which can be used is limited by the construction because the plugboard is located close to the front of the cover and not many cables can be accommodated in this narrow space. For this reason reccurse was also had to the permutation of the wheels. The three movable wheels can be shifted about in 3! ways, so that with reference

to the initial sequence five new sequences are possible. But each new sequence virtually signifies a new period of some 17,000 steps so that for one day we should have available a period of 104,000 steps, which was considered adequately secure if enough bridges were used. Naturally one also thought of inserting new wheels in the machine from time to time. That was the practice. Naturally provision was also made that the message key chosen in each case must be disguised before transmission in order not to make decipherment too easy for the enemy, because if he was already deciphering the traffic he would then have to fuss around with the messages before he recognized the affinity of messages belonging together. And in the opinion of Chi this would as a rule have required so much time that he could not gain any immediate tactical use from the messages solved. More was not asked for.

8) Beyond that there were naturally also theoretical studies which reached their climax by posing the question whether a single Enigma message can be solved if the machine is known and the keying instructions are known. Analytically this question was answered in the affirmative; I intentionally avoid saying "theoretically" because correct theory also has correct practice as a result or else there is an error in the theory or in the practice. And the answer ran that the individual Enigma message can be solved if I have the proper machine in my hands; the wheel position and all other settings may be unknown to me, I simply have to have in my hands a machine containing the wheels actually used. But what was carried out in this simplified experiment would in actual work have required a vast number of people or a gigantic battery of machines (mechanical aids to decipherment) so that under normal circumstances one could not count on any practical use /of the messages7.

Since I have not occupied myself with these matters for a very long time I can only give a few leading ideas today. If it is assumed that I have the machine actually used and messages enciphered on this machine, it may be assumed, let us say, that in one of the messages the word

"Regiment" occurs. Now the attempt may be made of writing every 8 successive letters of the cipher text beneath the plain text; the Enigma would then have to be stepped until at the proper point in the cipher text it gave the plain text, "Regiment", and it would also have to give rational text before and after this word. It is clear that such a task would not only call for a great deal of effort but would also cost time. And if this vast expenditure really did bring success, then with a new message, a new wheel setting and new plug connections, the game would begin all over again! Chi told itself that in a modern war one cannot reckon with such loss of time in deciphering - and therefore regarded the machine as adequately secure, if correctly handled.

Another method, which is more clever, started with the fact that the most frequent letter in German is E. Hence if I write out two messages in the same key, one below the other, then there will always be two like letters one below the other and of these a not inconsiderable portion will correspond to plain E. Working from the weak point, the next step was to assume that in German an N is likely to follow E. Again it was necessary to fuss around with the machine until most of these assumptions proved correct. But even in this case the loss of time and energy is so great that it stands in no rational relation to the expected results, always assuming that current reading of the messages will not be made possible by either of the methods. I can no longer go into detail regarding the very clever study. The individual lines of reasoning are likewise so complicated for me that I should only feel safe if I could regain the fresh impression. But after years spent in other work and in view of the fact that I only engaged in the early stage of these studies, while they were later taken over by others who could devote themselves exclusively to investigating such problems, both my memory and my imagination fail me today, without the device at hand, when I attempt to reconstruct the several operations in such vivid and truthful fashion as to enable me to give the exact course of solution.

9) The only disadvantage of the little Hagelin, for instance the B-211, is that it turns out the cryptograms much too slowly to satisfy present-day demands for speed. In comparison with the Enigma it has the advantage of being considerably smaller, of having a period which far exceeds that of the Enigma, - I believe it is around 3,000,000 steps, the exact number would have to be computed using the model. Whereas in the case of the Enigma the course of the period is always constant in small portions in spite of the rests (Rasten), the pin wheels of the Hagelin provide for an unsteady run-off of the period, if we conceive of the single step sequences as a function of a normal period. Through the riders, especially if they are all easily moved, an additional easily handled variant is introduced into the rigid system, which is stronger than in the case of the Enigma. Hence, in spite of certain similarities in idea and even constructional kinships the Hagelin represents an essential improvement of a substitution system in comparison with the Enigma: the Hagelin is the more modern device anyway; developed and built when the early experience with the Enigma was available; the Enigma nevertheless still has the distinction of having been the first cipher machine which was put into practical use and satisfied modern security demands. It is characteristic of both machines that when used improperly they yield messages which can be solved if in volume; however, this is not an organic fault but an evil which can be avoided without further ado if the machine is expertly handled. Hagelin's machine does not work with reciprocal alphabets.

17. Were you consulted on cryptographic security studies, investigations, and records made by HUETTENHAIN? What became of these studies?

Y[illegible]ired repeatedly. These studies must have been burned either in Berlin or in Halle or Werfen according to orders. No lists were made and no reports of destruction were submitted.

18. What do you know of MENZER's Schluesselscheibe and Schluesselkasten? Can you describe their method of encipherment?

I assume the following to be known:

DF 187-G

1. Use of double transposition and similar transposition systems in the German Army after World War I,
2. Use of the Enigma with lamps in the German Army after World War I,
3. The theoretical and material advantages and disadvantages of Systems 1 and 2.

The criticisms made during almost twenty years in numerous conferences, courses and discussions pursued the goal of creating for the use of troops not equipped with cipher machines a device possessing the following qualities:

a. Light weight and small size

b. Trouble sources - none

c. Ease of operation

d. Derivation of the secret or plain text by some simple rule, in any event by one operation

e. Security of the secret texts against cryptanalysis

f. Simple distribution of keys

g. Simple administration

None of the hand systems, however clever, satisfied these conditions. (The very intriguing French small signal table with approximately 1,000 entries and with numerous blank groups for ad hoc and ad libitum entries was excellent, as experience had shown, but called for an organization with extensive printing and distributing facilities). For this reason some other course had to be taken. Numerous proposals made by lay inventors for the use of linear or disc slides had to be rejected as unserviceable, even when - to increase cryptographic security - the secret text became a function of the plain text. For precisely in these cases an error in encipherment continues as a function throughout the entire telegram. The only idea which proved of theoretical and practical value on the basis of numerous experiments was the use of a substitution system with a periodic course but with a long period. The technical problem was therefore to mechanize this idea. For reflection shows that even with a primitive linear slide

```
Plain   m y l u n b s h v t a l x d q j g r k c p z f w o e
Cipher  p u c i v d z n q o r a m y j b w x f s k e l h t g p u c i v d z n q o
```

and an aperiodic numerical key, for instance 4 1 3 2 0 3 1 5 2 6 4 1 0 .... 4 3 1 0 3 a cryptogram can be derived for which analysis can indicate no solution although it goes back to the Middle Ages, (to Tritheim, according to Blaise de Viginere, born 9.2.1462, died 16.12.1516).

If it were possible to employ a virtually infinite and aperiodic digit sequence to derive the red slide, then in effect the desired device would be created.

The minimum length of such a device had its natural limits however: if the alphabets were to be interchangeable, then the cells must be capable of inscription. Using cells one cm wide would have given a length of 52 cm or more, due to the doubling of the one alphabet. However, this could not be thought of! A way out of the difficulty was found by dividing both alphabets in the following manner:

M	Y	I	U	N	B	S	H	V	T	A	L	X													
P	U	C	I	V	D	Z	N	Q	O	R	A	M	P	U	C	I	-	-	.	-	-	-	-	-	M
Y	J	B	W	X	F	S	K	E	L	H	T	G	Y	I	B	W	-	-	.	-	-	-	-	-	G
D	Q	J	G	R	K	C	P	Z	F	W	O	E													

With such an arrangement the device could be reduced to a total length of about 30 cm. But a disadvantage, the effects of which were not yet known, was the coupling of two black and two red letters in each case. The working out of the drive mechanism was more difficult in such a limited space.

A spring supplied the driving power. It was released by a push button. When at rest the movable slide had to be firmly blocked. The final step of the slide, which was drawn out by hand each time, could not be ambiguous. Consequently great mechanical precision was required everywhere in the device.

To mechanize the aperiodic course, recourse was had to so-called pin wheels (Bolzenraeder), such as are used to achieve the same goal in the Hagelin device, and to the requisite gear [illegible] elements were so conveniently reached from the bottom of the device that even the clumsy finger of a soldier could service the individual parts.

I no longer know how many gear wheels and how many pin wheels the device had. But four gear wheels with 17, 19, 21 and 23 teeth would already give a period of 156,009 steps. I assume that at least five gear wheels were envisioned and probably a like number of pin wheels, but this is not essential.

DF 187-G

The effect of the pin wheels is naturally to shorten the total period. Likewise there are favorable and unfavorable pin positions. The problem of the favorable pin positions was the subject of special speculation. And in practical use every cipher clerk would have to have a table showing the "forbidden" pin settings. This table had already been computed at OKW/Chi.

An experimental Menzer Slide (Menzerschiebe) about 17 cm long, about 8 cm wide and about 6 cm high had been built, but with a much shorter period. The Wanderer-Werke had been entrusted with manufacture. The Army never got beyond the stage of experimental devices. At least I never heard that even a first set of these devices reached a try-out with the troops. All the experimental models suffered from the fact that the device was always jamming and therefore was of no practical use.

In practical use the following rules were to be observed:

1. A completely new inscription at least once a day,

2. A new pin setting and gear setting for each message.

The choice of these two elements should be left to the code clerk so as to guarantee as individual use as possible. Of course these data had to be given in each message by an indicator group. I never saw any completed book of instructions or directions for use.

In my opinion the device satisfied the demands for temporary cryptographic security but to my knowledge no definitive analytical study had as yet been completed.

19. In the Schluesselkasten is the slide returned after each encipherment or only when necessary?

I do not know this system or at any rate no longer have it in mind. However, any necessary aids for encipherment and decipherment cannot possibly be returned as soon as the job is [illegible] cipher is involved, then there would be no possibility of returning it! To whom, for instance, should part of the cryptographic system of German agents in Sweden be turned in? From the way the question was put I believe I can assume that the entire principle of the Schluesselkasten is still in need of clarification.[14]

III. SECRET INKS AND MICROPHOTOGRAPHY

20. What do you know about secret ink and microphotography?

I do not understand anything about serious secret inks and know no more than can be found in any "Book of Magic" for boys or in any encyclopedia. Secret inks were solely of concern to the Abwehr. Likewise microphotography. Just once, when I was getting some acetone at the Abwehr laboratory I looked through a microscope and recognized a map of Germany in what to the naked eye looked like an ordinary period. Why it had been made I do not know. It was shown to me simply to prove how capable microphotography is.

In the First World War a white powder, of which I do not know the composition, was dissolved in ordinary water. One wrote with this solution on a paper which would take ink. As soon as the ink was dry, the writing was gone over with a solution of sal ammoniac. Upon development the writing was supposed to come out if the paper was immersed in a dilute solution of acetic acid. During the First World War it was claimed, as a rule, that a secret ink must be so constituted as to be utterly destroyed chemically if the enemy attacked it with a bleach; or: use such bleaches as will not destroy any writing that may be present. Whether this notion has any validity today, when a multitude of otherwise invisible substances can be revealed by quartz lamps, is beyond my knowledge.

[14] FENNER's answer was based apparently on a mistranslation by the interrogator of the word "returned" which was rendered "zurueckgegeben" or "given back" whereas some such term as "zurueckgezogen" = "pulled back" or "zurueckgeschoben" = "shoved back" /i. e., to the "initial position"/ was intended.